Please type a plus sign (+) inside this box → ☐ +

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.	10209-00007
First Named Inventor or Application Identifier	Eugene August Fusz
Title	METHOD AND APPARATUS FOR ANONYMOUS DATA PROFILING
Express Mail Label No.	EL319727354US

APPLICATION ELEMENTS
See MPEP chapter 600 concerning utility patent application contents.

ADDRESS TO: Assistant Commissioner for Patents
Box Patent Application
Washington, DC 20231

1. [X] Fee Transmittal Form *(e.g., PTO/SB/17)*
   (Submit an original, and a duplicate for fee processing)

2. [X] Specification — *[Total Pages]* 14
   (Preferred arrangement set forth below)
   - Descriptive title of the Invention
   - Cross References to Related Applications
   - Statement Regarding Fed sponsored R & D
   - Reference to Microfiche Appendix
   - Background of the Invention
   - Brief Summary of the Invention
   - Brief Description of the Drawings *(if filed)*
   - Detailed Description
   - Claim(s)
   - Abstract of the Disclosure

3. [X] Drawing(s) *(35 USC 113)* — *[Total Sheets]* 4

4. Oath or Declaration — *[Total Pages]* 2
   a. [X] Newly executed (original or copy)
   b. [ ] Copy from a prior application (37 CFR 1.63(d))
      (for continuation/divisional with Box 17 completed)
      [Note Box 5 below]
      i. [ ] **DELETION OF INVENTOR(S)**
         Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).

5. [ ] Incorporation by Reference *(useable if Box 4b is checked)*
   The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.

6. [ ] Microfiche Computer Program *(Appendix)*

7. Nucleotide and/or Amino Acid Sequence Submission
   (If applicable, all necessary)
   a. [ ] Computer Readable Copy
   b. [ ] Paper Copy (identical to computer copy)
   c. [ ] Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

8. [ ] Assignment Papers (cover sheet & document(s))
9. [ ] 37 CFR 3.73(b) Statement *(when there is an assignee)* — [X] Power of Attorney
10. [ ] English Translation Document *(if applicable)*
11. [ ] Information Disclosure Statement (IDS)/PTO-1449 — [ ] Copies of IDS Citations
12. [ ] Preliminary Amendment
13. [X] Return Receipt Postcard (MPEP 503) *(Should be specifically itemized)*
14. [X] Small Entity Statement(s) (PTO/SB/09-12) — [ ] Statement filed in prior application, Status still proper and desired
15. [ ] Certified Copy of Priority Document(s) *(If foreign priority is claimed)*
16. [X] Other: EXPRESS MAIL CERTIFICATE

NOTE FOR ITEMS 1 & 14: IN ORDER TO BE ENTITLED TO PAY SMALL ENTITY FEES, A SMALL ENTITY STATEMENT IS REQUIRED (37 C.F.R. §1.27), EXCEPT IF ONE FILED IN A PRIOR APPLICATION IS RELIED UPON (37 C.F.R § 1.28).

17. If a CONTINUING APPLICATION, check appropriate box and supply the requisite information:
    [ ] Continuation   [ ] Divisional   [ ] Continuation-in-part (CIP)   of prior application No:
    Prior applicaton information: *Examiner:*   *Group/Art Unit:*

18. CORRESPONDENCE ADDRESS

[ ] Customer Number or Bar Code Label
(Insert Customer No. ar Attach bar code label here)   or   [ ] Correspondence address below

NAME	John S. Beulick
	Armstrong Teasdale LLP
ADDRESS	Suite 2600
	One Metropolitan Square
CITY	St. Louis
STATE	MO
ZIP CODE	63102
COUNTRY	U.S.A.
TELEPHONE	314/621-5070
FAX	314/621-5065

Name (Print/type)	Patrick W. Rasche	*Registration No. (Attorney/Agent)*	37,916
Signature	*Patrick W. Rasche*	*Date*	10/26/99

CERTIFICATE OF MAILING BY EXPRESS MAIL TO
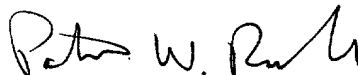## THE COMMISSIONER OF PATENTS AND TRADEMARKS

Express Mail mailing label number: **EL319727354US**

Date of Mailing: <u>October 26, 1999</u>

    I certify that the attached complete utility patent application of **Eugene August Fusz for METHOD AND APPARATUS FOR ANONYMOUS DATA PROFILING,** including:

- Patent Application Transmittal (1 page)

- Fee Transmittal (in duplicate) (1 page)

- Eight (8) pages of specification; five (5) pages of claims; one (1) page of abstract

- Four (4) sheet of drawings

- Declaration and Power of Attorney (2 pages)

- Statement (Declaration) Claiming Small Entity Status (37 CFR 1.9 (f) and 41 (a) and 1.27 (b)) - Independent Inventor (2 pages)

- Certificate of Mailing Via Express Mail (1 page)

- Return post card

is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 C.F.R. §1.10 on the date indicated above in an envelope addressed to Box Patent Application, Assistant Commissioner for Patents, Washington, D.C. 20231.

Patrick W. Rasche
Reg. No. 37,916
Armstrong Teasdale LLP
One Metropolitan Square, Suite 2600
St. Louis, MO 63102
    314/621-5070

Applicant or Patentee: Eugene August Fusz_____
Serial or Patent No.: _____
Filed or Issued: _____
For: METHOD AND APPARATUS FOR ANONYMOUS DATA PROFILING_____

STATEMENT (DECLARATION) CLAIMING SMALL ENTITY STATUS
(37 CFR 1.9 (f) and 41 (a) and 1.27 (b)) - INDEPENDENT INVENTOR

As a below named inventor, I hereby declare that I qualify as an independent inventor as defined in 37 CFR 1.9(c) for purposes of paying reduced fees under section 41(a) and (b) of Title 35, United States Code, to the Patent and Trademark Office with regard to the invention entitled METHOD AND APPARATUS FOR ANONYMOUS DATA PROFILING described in:

      [✓] the specification filed herewith
      [ ] application serial no. _____, filed _____.
      [ ] patent no. _____, issued _____.

I have not assigned, granted, conveyed or licensed and am under no obligation under contract or law to assign, grant, convey or license, any rights in the invention to any person who could not be classified as an independent inventor under 37 CFR 1.9(c) if that person had made the invention, or to any concern which would not qualify as a small business concern under 37 CFR 1.9(d) or a nonprofit organization under 37 CFR 1.9(e).

Each person, concern or organization to which I have assigned, granted, conveyed, or licensed or am under an obligation under contract or law to assign, grant, convey, or license any rights in the invention is listed below:

      [✓] no such person, concern, or organization
      [ ] persons, concerns or organizations listed below*

      *NOTE: Separate verified statements are required from each named person, concern or organization having rights to the inventions averring to their status as small entities. (37 CFR 1.27).

FULL NAME EUGENE AUGUST FUSZ_____
ADDRESS 925 North Lindbergh, St. Louis, MO 63141_____

    [✓] INDIVIDUAL   [ ] SMALL BUSINESS CONCERN   [ ] NONPROFIT ORGANIZATION

I acknowledge the duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small entity is no longer appropriate. (37 CFR 1.28(b))

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this verified statement is directed.

EUGENE AUGUST FUSZ		
NAME OF INVENTOR	**NAME OF INVENTOR**	**NAME OF INVENTOR**
Signature of Inventor	Signature of Inventor	Signature of Inventor
10/26/99		
Date	Date	Date

METHOD AND APPARATUS FOR ANONYMOUS
DATA PROFILING

BACKGROUND OF THE INVENTION

This invention relates generally to methods for gathering information, and more particularly to methods and apparatus for anonymous data profiling of consumers.

One well accepted marketing tool is to gather information about a target audience and direct a product, or service, to that audience. However, it is difficult to obtain information about the target audience because many individuals do not freely provide information about themselves to strangers. One reason is because the more information people divulge about themselves, the more likely it is that others will use that information to contact the person that divulged the information.

Accordingly, it would be desirable to provide companies with targeted information while not divulging personal contact information of the consumer.

BRIEF SUMMARY OF THE INVENTION

In an exemplary embodiment, a method for gathering anonymous data about an individual includes administering a password to the individual, receiving information from the individual, and storing the information in a database. Identifiers such as name, address and social security number are not included in the gathered anonymous data.

The anonymous data includes a number of attributes. The attributes are compared with marketer generated data sets to determine if the marketer generated data sets would possibly be a match with the individual's attributes. If a match is determined, then the market generated data sets are permitted to reach the consumer. The consumer is then given the opportunity to provide feedback to the system to enrich the marketer data set. Thus individuals may provide valuable feedback to marketers without divulging identifying information about themselves.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a block diagram of an exemplary embodiment of a server architecture for a consumer generated anonymous data system;

Figure 2 is a block diagram of an alternative exemplary embodiment of a server architecture for a consumer generated anonymous data system;

Figure 3 is a schematic diagram of a method for generating anonymous data profiles of individuals; and

5   Figure 4 is a schematic diagram of a method for utilizing anonymous data profiles to respond to marketing generated data sets.

DETAILED DESCRIPTION OF THE INVENTION

Figure 1 is a block diagram of an exemplary embodiment of a server architecture for an electronic data communications network system 10 that gathers and utilizes consumer generated anonymous data. System 10 is connected to a distributed computer network, such as the Internet, including that part of the Internet known as the World Wide Web. The term Web as used herein refers to the World Wide Web, wherein computers known as Web servers display graphical and textual information using files or "pages" composed in Hyper Text Mark-up Language (HTML). The Web servers communicate information over the Web or other network from a Web server at a central site to a remote computer terminal used by a customer. Although the exemplary system described herein is implemented on the Web, it should be understood that other types of distributed computer networks are suitable for being connected to system 10.

In one embodiment of system 10, the location of a page on the Web is specified by a uniform resource locator (URL), which is an alphanumeric string representing the server address on the Web. At the remote computer terminal, a remote user initially accesses a page by typing a specified URL into a Web-browser such as Netscape™ by Netscape Communications Corporation, or Internet Explorer™ by Microsoft Corporation. Multiple pages at a Web site are linked together via hyperlinks which are represented on a computer screen by a graphical icon such as a button or a highlighted line of text. Hyperlinks are configured to implicitly invoke another URL when a computer user clicks on a computer mouse button while a mouse-controlled screen cursor is positioned over a hyperlink icon.

In one embodiment, as shown in Figure 1, system 10 includes a web server 12, an application server 14, a database server 16, a directory server 18, a workflow server 20, and a mail server 22. A disk storage unit 24 is coupled to

database server 16 and directory server 18 and provides a data repository for storing data pertaining to consumer generated anonymous data and marketer generated data. Servers 12, 14, 16, 18, 20 and 22 are coupled in a local area network (LAN) 24. LAN 24 also includes a processor (not shown) programmed to communicate with servers 12, 14, 16, 18, 20, and 22.

Web server 12 and mail server 22 are configured to be communicatively coupled to computers 26, 28, and 30 of individuals, i.e., consumers, via an ISP Internet connection 32. In addition, a plurality of computers 34, 36, 38, and 40 of marketers are communicatively coupled to web server 12 and mail server 22 via ISP Internet connection 32. Further, at least one work station 42 is coupled to LAN 24 for simultaneous monitoring of various tasks and methods described below. The processor is further programmed to communicate with consumer computers 26, 28, and 30, with marketer computers 34, 36, 38, and 40, and with work station 42.

The communication in the exemplary embodiment is illustrated as being performed via the Internet through web browsers loaded onto computers 26, 28, 30, 34, 36, 38, and 40 of consumers and marketers, respectively. Other wide area networks (WAN), however, could be used in other embodiments, i.e., the systems and processes described herein are not limited to being practiced over the Internet. LAN 24 is configured to store data obtained through an interface (not shown) such as a web page maintained on web server 12, to compare data generated by consumers with data generated by marketers, and to enable consumers to access selected sets of information generated by marketers.

Figure 2 is a block diagram of an alternative exemplary embodiment of a server architecture for a system 50 that gathers and utilizes consumer generated anonymous data. Components in system 50 identical to components of system 10 are identified in Figure 2 using the same reference characters as in Figure 1. System 50 differs from system 10 in that system 50 includes a fax server 52 coupled to LAN 24. Fax server 52 communicates with consumers via a telephone link 54. Also, in system 50 the mail server is incorporated into web server 22.

The architecture of systems 10 and 50 are exemplary only. Other architectures are possible and can be utilized in connection with practicing the methods described below. Moreover, the methods described below could alternatively be initiated by a consumer without a computer or fax machine. For example, customers could phone or mail the required information and an operator

could enter data directly into LAN 24 by workstation 42 or by an operator with a computer remotely communicating with LAN 24 through ISP Internet Connection 32 or other WAN.

Figure 3 is a schematic diagram of a method 100 for generating anonymous data profiles about a consumer. Method 100 includes the step of accessing 102 a consumer generated anonymous data system, such as systems 10 and 50 shown in Figures 1 and 2, respectively. Access to consumer generated anonymous data systems 10 and 50 is through a secure access that entitles only a limited number of individuals to enter systems 10 and 50. As described below in greater detail, the information supplied by the individuals is considered to be confidential proprietary information. To protect the information from unauthorized individuals seeking access, the system includes a security element. One example of such a security element is a firewall.

The firewall is a software-based gateway which impedes or limits access to a LAN, such as LAN 24 shown in Figures 1 and 2. The access is machine-limited so that only authorized remote computers have permission to get through the firewall. To implement the firewall, the system in one embodiment includes servers, such as web server 12 shown in Figures 1 and 2, mail server 22 shown in Figure 1, or fax server 52 shown in Figure 2, through which all communications with computers outside LAN 24 must take place. Servers 12, 22, and 52 are programmed to validate queries from a user on any machine authorized to communicate with LAN 24 via remote terminals, such as terminals 26, 28, 30, 34, 36, 38, 40, and 42. Servers 12, 22, and 52 include special programs enabling them to forward valid requests or queries from authorized machines through the firewall to LAN 24.

Alternatively, the security element identifies authorized users rather than machines. This approach is more complex than the basic firewall approach because queries or requests from a user on any remote terminal are validated using an encrypted unique identifier inputted at the remote terminal. The unique identifier is, e.g., a password such as a validation code consisting of an alphanumeric string. Alternatively, the password can be combined with answers to a series of questions. The unique identifier is encrypted to frustrate password sniffers who are capable of intercepting unencrypted passwords as they pass from machine to machine through the Web. Servers 12, 22, and 52 validate the encrypted unique identifier, and allow access to LAN 24. In another alternative embodiment, the security element identifies

authorized users using a one-time or limited use password supplied by servers 12, 22, and 52 on request from the user.

In one exemplary embodiment, a first time a user accesses the consumer generated anonymous data system, the user is requested to create 104 a multi-character identifier password. After an appropriate password has been created, the user is then requested 106 to answer a series of questions. Alternatively, the user chooses a series of questions and answers those questions accordingly. The questions are personal questions that invoke answers specific to the user. An exemplary question is "favorite color". After the personal questions have been answered, the user is granted access 108 to LAN 24. Once LAN 24 has been accessed, the user is provided access 110 to a consumer generated anonymous data database. The user is then requested to fill out 112 a detailed questionnaire as described below in greater detail. The answers to the questions in the questionnaire are stored 114 in a consumer generated anonymous data database. When the user decides to leave 116 the database and the LAN, the user exits the consumer generated anonymous data system.

If the user decides to return to the consumer generated anonymous data system, the user again accesses 102 the consumer generated anonymous data system and is requested to submit 118 the user's password. If the correct password is submitted, the user is then requested to answer 120 a question specific to the user identified by the password. Each question is asked only one time, or a limited number of times, per visit, or per day, to reduce the possibility of someone other than the user correctly answering the questions. In addition, all communications between the user and the consumer generated anonymous data system are encrypted to provide additional security measures to method 100.

If the user answers the question correctly, the user is granted access to the LAN as described above. If the user answers the question incorrectly, the user is requested to answer a second question. If the user answers the second answer correctly, the user is granted access to the LAN. If, however, the user answers the second question incorrectly, the user is requested to answer a third question. This question and answer session continues until either the user correctly answers a question, or the system exhausts its list of questions. If no correct answers are given, the user is denied access to the system. In an alternative embodiment, if the user incorrectly answers the first question, the user is denied access to the system for a remainder of the day.

When access is granted to the user, all communications between the user and the consumer generated anonymous data system are conducted utilizing the password. The user is directed to supply no contact information to the system. Such information includes, but is not limited to, name, address, social security number, and telephone number. The lack of this contact information in the consumer generated anonymous data database adds a further layer of privacy to the information supplied by the user to the system. This supplied information may then be utilized by the system, while the user's identity is maintained in confidence by the user. The system never has access to the user's identity.

The consumer profile is generated using the questionnaires. A series of questionnaires will be presented to the consumer. Each questionnaire will take the consumer about 10 – 15 minutes to complete. The questions will be formatted, for example, as multiple choice, true/false, or short answer. The first questionnaire will be general in nature, and will include questions directed, for example, to categories such as age, sex, marital status, zip code, number, sex, and ages of children, spouse, job, residence, pets, hobbies, cars, and others. Follow-up questionnaires will include questions directed towards answers given in the initial, or previous, questionnaires.

Figure 4 is a schematic diagram of a method 150 for providing feedback regarding sets of marketing data utilizing anonymous consumer data profiles. The anonymous consumer generated data profiles are generated and stored as explained above with respect to Figure 3. After the profiles are generated, a consumer generated anonymous data system, such as one of systems 10 and 50 shown in Figures 1 and 2, respectively, accepts marketer generated data, i.e., advertising data, in a marketer data base, as described below. An administrator, or intermediary, oversees the consumer generated anonymous data system and is the point of contact for the marketers and for the consumers. Thus, the marketers have no contact with the consumers.

A company that desires to have consumer feedback on one or more products or services accesses 152 the consumer generated anonymous data system via a URL. The company then requests 154 to have a set of data reviewed by a relevant group of consumers. The sets of data may be, for example, an advertisement or other information on which the company would like to obtain feedback. The company agrees 156 to provide compensation in return for feedback from the relevant group of consumers. The compensation is paid to the intermediary, who then distributes a

portion of the compensation to the consumers, as described below in greater detail. The set of data is then stored 158 in a marketer database. The set of data is reviewed 160 by the system to determine 162 the relevant group of consumers. For example, the consumer generated anonymous data system includes a processor programmed to

5   compare the set of data with each consumer generated profile to determine which individual consumers may be interested in viewing the set of data.

After the processor has determined which consumers may be interested in viewing the set of data, a record is made 164 of those consumers. When each consumer accesses the consumer generated anonymous data system, those consumers

10   on the record are notified 166 of a potentially relevant set of data that may be of interest to them. If the consumer views 168 the set of data, the consumer is given the opportunity to provide 170 feedback to the system with respect to that set of data. The feedback provided by the consumer will include information regarding whether the consumer approved or disapproved of the set of data. In addition, the feedback

15   will include information regarding whether the consumer has any interest in viewing similar sets of data in the future, and whether the timing for viewing similar sets of data is appropriate. The system will thus be able to better match consumers with sets of data based on the feedback provided by the consumers. The feedback that is directed towards the approval or disapproval of the set of data will be aggregated by

20   the intermediary and then provided to the company. In addition, the feedback will be broken down in a detailed format.

The consumer then receives 172 compensation for providing feedback with respect to the set of data. In an exemplary embodiment, the compensation is in the form of digital cash, online credits, or a coupon issued to the user. The coupon

25   can be printed by the user and taken to a designated bank, savings and loan, or credit union which will then cash the coupon. The user thus maintains their anonymity and is still able to be compensated for their time to provide feedback regarding the sets of data they reviewed.

Although the company can access the consumer generated anonymous

30   data system, the company is unable to access the consumer generated anonymous data database. Access to the consumer generated anonymous data database is only permitted if a correct password and answers to a series of questions is given. Therefore, the company does not have access to any of the consumer generated

anonymous data other than that provided by the intermediary regarding the aggregated information of the consumers.

The LAN and the consumer generated anonymous data system are operated by an intermediary. The intermediary sorts and organizes the data entered by the consumers and also the data entered by the companies. In addition, the intermediary matches the correct set of data to be reviewed with the relevant individual to review the data. The intermediary also forwards the appropriate compensation to the appropriate individual after their review of an ad.

The consumer generated anonymous data system and the method for generating anonymous data profiles provides an extra level of security to individual consumers. The consumers can freely divulge information without anyone knowing who provided the information. The system allows the consumer to create a self-generated profiling data set that is rich in content, yet anonymous. Because of the rich content of the data set, the system provides efficient target marketing to companies. Thus, companies get aggregated feedback from a targeted audience and consumers can provide insight into products and services while keeping their identities from the companies.

While the invention has been described in terms of various specific embodiments, those skilled in the art will recognize that the invention can be practiced with modification within the spirit and scope of the claims.

WHAT IS CLAIMED IS:

1. A method for generating an anonymous data profile of an individual, said method comprising the steps of:

administering to the individual a password;

utilizing the password to access a database;

5   entering information about the individual in the database; and

storing the information from the individual in the database.

2. A method in accordance with Claim 1 wherein said step of administering to the individual a password comprises the step of allowing the individual to choose a multi-character identifier.

10   3. A method in accordance with Claim 1 wherein said step of administering to the individual a password comprises the step of asking the individual a plurality of questions.

4. A method in accordance with Claim 2 further comprising the step of communicating with the individual via the password.

15   5. A method in accordance with Claim 4 wherein said step of communicating with the individual comprises the step of asking the individual for the multi-character identifier.

6. A method in accordance with Claim 5 wherein said step of communicating with the individual further comprises the step of asking the individual
20   at least one personal question, wherein the individual is permitted to enter the database only if the correct multi-character identifier is given and if at least one of the personal questions is answered correctly.

7. A method in accordance with Claim 1 wherein said step of receiving information from the individual comprises the step of receiving information excluding
25   a name, a social security number, and an address of the individual.

8. A method for providing advertising feedback, said method comprising the steps of:

administering to each individual a password;

utilizing the password to access a database;

entering information about the individual in the database;

storing the entered first set of information in the database;

presenting at least one of the individuals with a second set of information; and

receiving feedback from the at least one individual regarding the second set of information.

9. A method in accordance with Claim 8 wherein said step of presenting each individual with a second set of information comprises the step of presenting each individual with a second set of information generated by an advertiser.

10. A method in accordance with Claim 8 further comprising the step of communicating the feedback in aggregate form to the advertisers.

11. A method in accordance with Claim 8 wherein said step of administering to each individual a password comprises the step of allowing each individual to choose a multi-character identifier.

12. A method in accordance with Claim 8 wherein said step of administering to each individual a password comprises the step of asking the individual a plurality of questions.

13. A method in accordance with Claim 8 further comprising the step of paying the individuals for their feedback.

14. A method in accordance with Claim 8 further comprising the step of separating the first set of information from the second set of information and ensuring the advertisers do not obtain the first set of information.

15. A method in accordance with Claim 8 wherein said step of presenting each individual with a second set of information comprises the step of

presenting each individual with a second set of information that is specific to the first set of information provided by the individual.

16. Apparatus for conveying and storing information relating to anonymous data profiles, said apparatus comprising:

a first data repository;

a first computer linked to said first data repository, said first computer configured to communicate with said first data repository via a password and provide a first set of information about an individual to said first data repository, the first set of information lacking information relating to a name, an address, and a social security number of the individual;

a processor programmed to communicate with said first data repository and said first computer.

17. Apparatus in accordance with Claim 16 wherein said processor is further programmed to store the first set of information from said first computer if a correct password is provided by said first computer.

18. Apparatus in accordance with Claim 16 further comprising:

a second data repository;

a second set of computers linked to said second data repository, said second set of computers configured to provide a plurality of second sets of information to said second data repository, said first data repository separate from said second data repository, said processor further programmed to communicate with said second data repository and said second set of computers.

19. Apparatus in accordance with Claim 18 wherein said second set of computers cannot access said first data repository.

20. Apparatus in accordance with Claim 18 wherein said processor is further programmed to screen the second set of information and grant access to the screened second set of information by the first computer if the screened second set of information includes at least one attribute compatible with at least one attribute in the first set of information.

21. Apparatus in accordance with Claim 20 wherein said first computer is configured to access the screened second set of information stored in said first data repository.

22. A system for generating and controlling anonymous data sets via an electronic data communications network, said system comprising:

a control unit for coupling to the communications network;

a server coupled to said control unit and comprising a consumer generated data base for storing information relating to consumers, a marketer data base for storing information to be reviewed by consumers, and a processor programmed to:

receive consumer generated data sets from consumers, said consumer generated data sets controlled by the consumers, each consumer generated data set including a set of individual characteristics, said processor further programmed to download said consumer generated data sets into said consumer generated data base;

receive information from marketers, said information controlled by said marketers, said processor further programmed to download said marketer generated data into said marketer data base;

said processor further programmed to compare said marketer generated data to each said consumer generated data set and if said marketer generated data is identified as matching one or more said individual characteristics of said consumer generated data sets, designating said marketer generated data for being communicated to the consumer.

23. A system in accordance with Claim 22 wherein said processor is further programmed to communicate said designated marketer generated data to the consumer if the consumer chooses to view said marketer generated data.

24. A system in accordance with Claim 23 wherein said processor is further programmed to communicate a consumer generated feedback of said designated marketer generated data to the marketer.

25. A system in accordance with Claim 22 wherein said processor is further programmed to prevent the marketers from accessing said consumer generated data sets.

5

26. A system in accordance with Claim 22 wherein said processor is further programmed to accept consumer generated data sets from the consumers if a correct password is received by said processor.

27. A system in accordance with Claim 22 wherein said consumer generated data sets do not include a name, an address, and a social security number of the consumer.

10

28. A system in accordance with Claim 22 wherein the electronic data communications network is a wide area network comprising the Internet.

10209-00007

METHOD AND APPARATUS FOR ANONYMOUS
DATA PROFILING

ABSTRACT OF THE DISCLOSURE

A method for gathering anonymous data about an individual includes administering a password to the individual, receiving information from the individual, and storing the information in a database. Contact information, such as name, address, telephone number and social security number are not included in the gathered anonymous data.

5

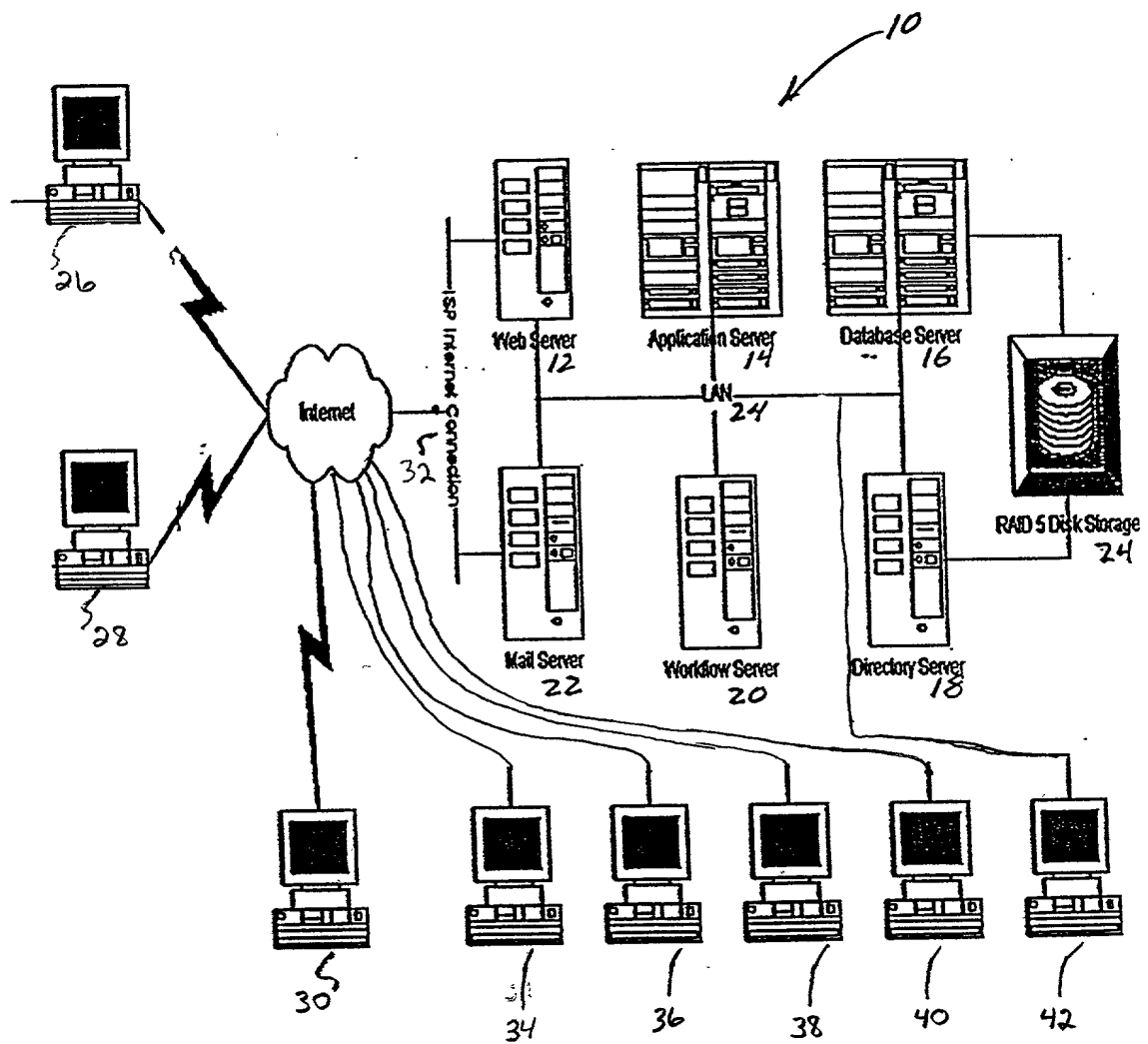ISP Internet Connection

Internet

Web Server
12

Application Server
14

Database Server
16

LAN
24

RAID 5 Disk Storage
24

Mail Server
22

Workflow Server
20

Directory Server
18

26

28

32

30

34

36

38

40

42

10

FIG. 1

FIG. 2

```
100

102  access the consumer
     generated anonymous
     data system

118  submit the
     appropriate password

120  answer a series of
     questions

104  create a new
     password

106  answer a series
     of personal questions

108  access the LAN

110  access the consumer
     generated data
     database

112  fill out a detailed
     questionnaire

114  store answers in a
     consumer generated
     anonymous data
     database

116  leave the LAN
```

FIG. 3

FIG. 4

150

152 — access consumer generated anonymous data system

154 — request consumer review of a set of data

156 — agree to provide compensation

158 — store the set of data

160 — review of set of data by system

162 — determine the relevant group of consumers

164 — record a list of relevant consumers

166 — notify relevant consumers of potentially relevant set of data

168 — view set of data by consumer

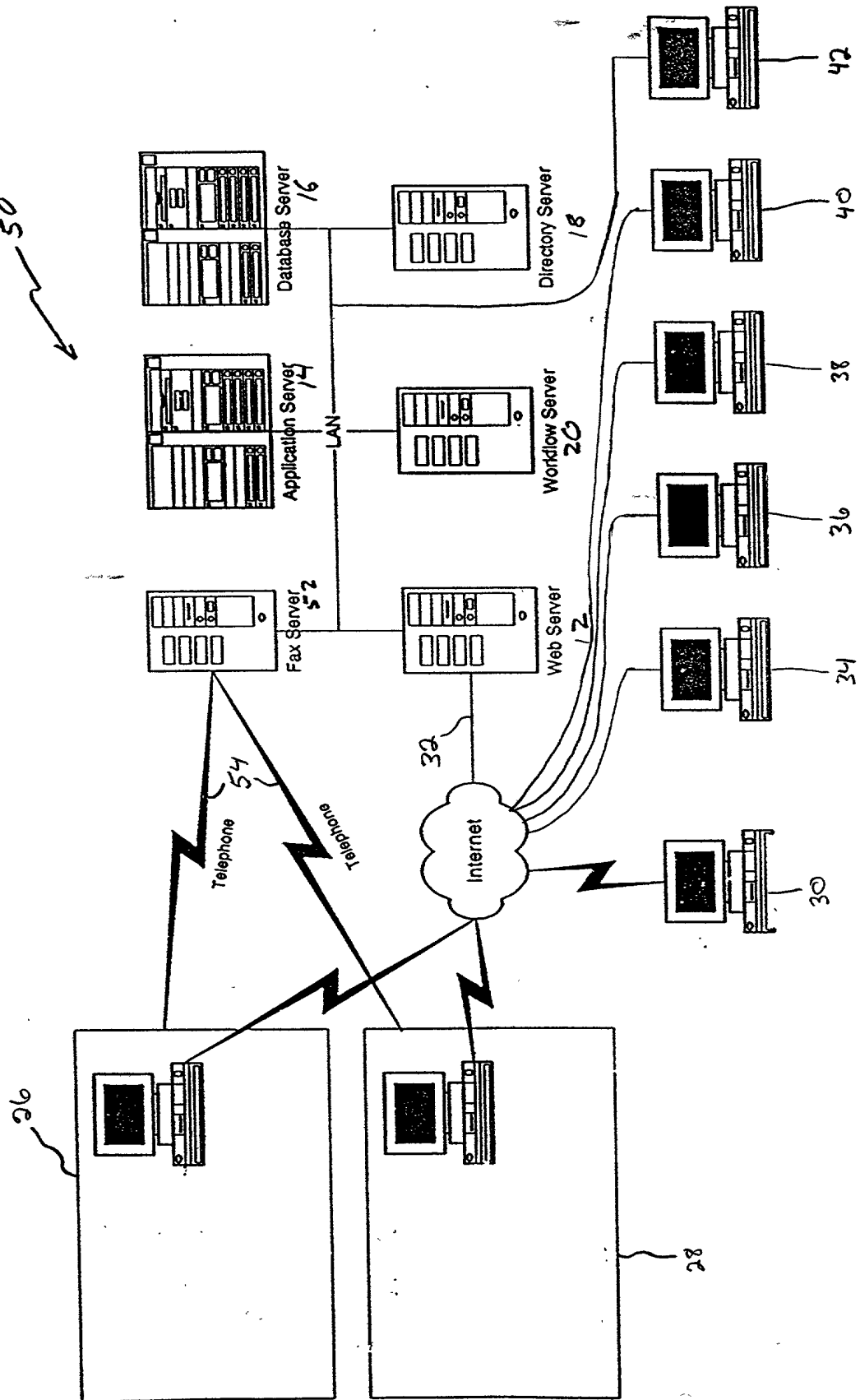170 — provide feedback to system
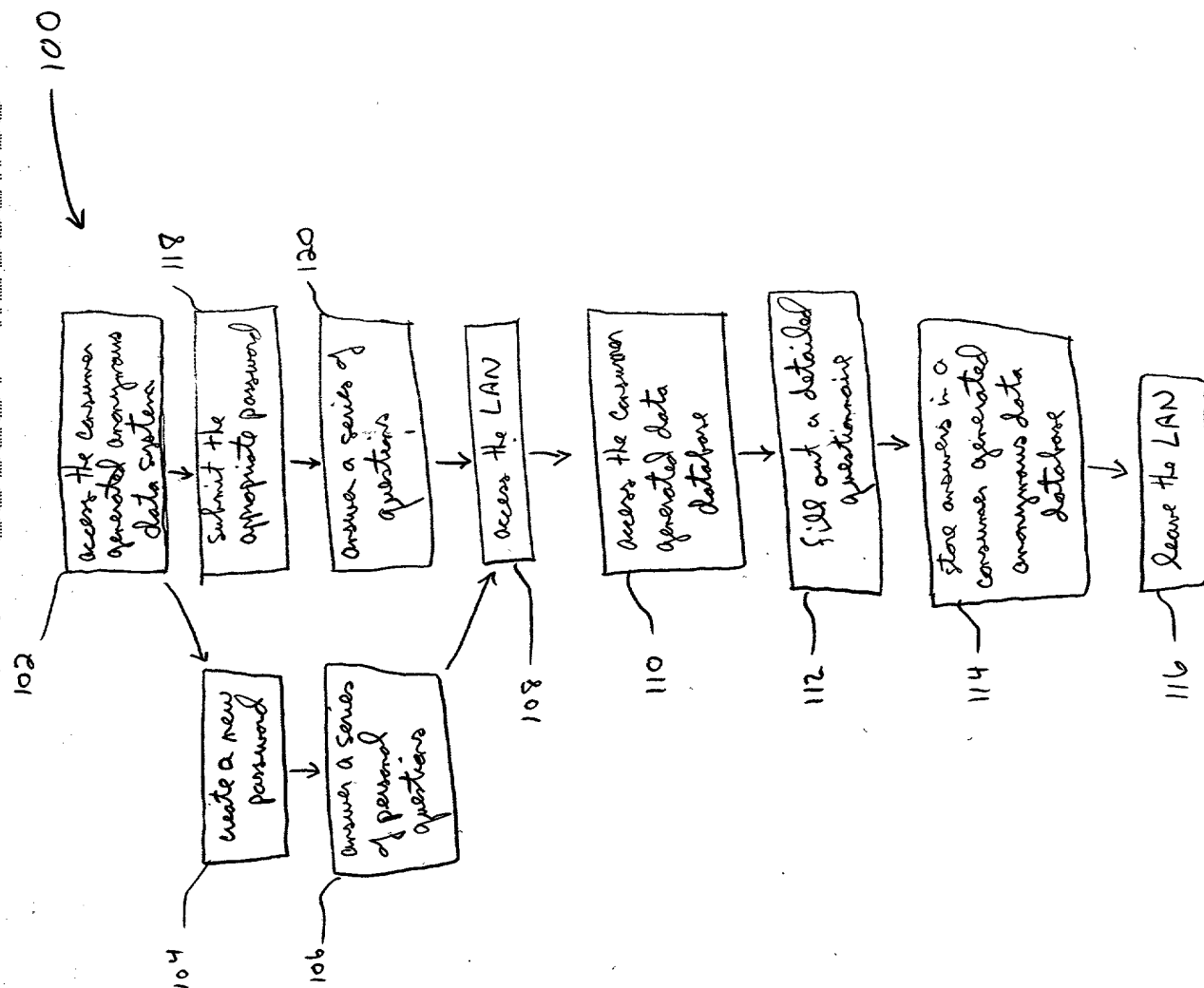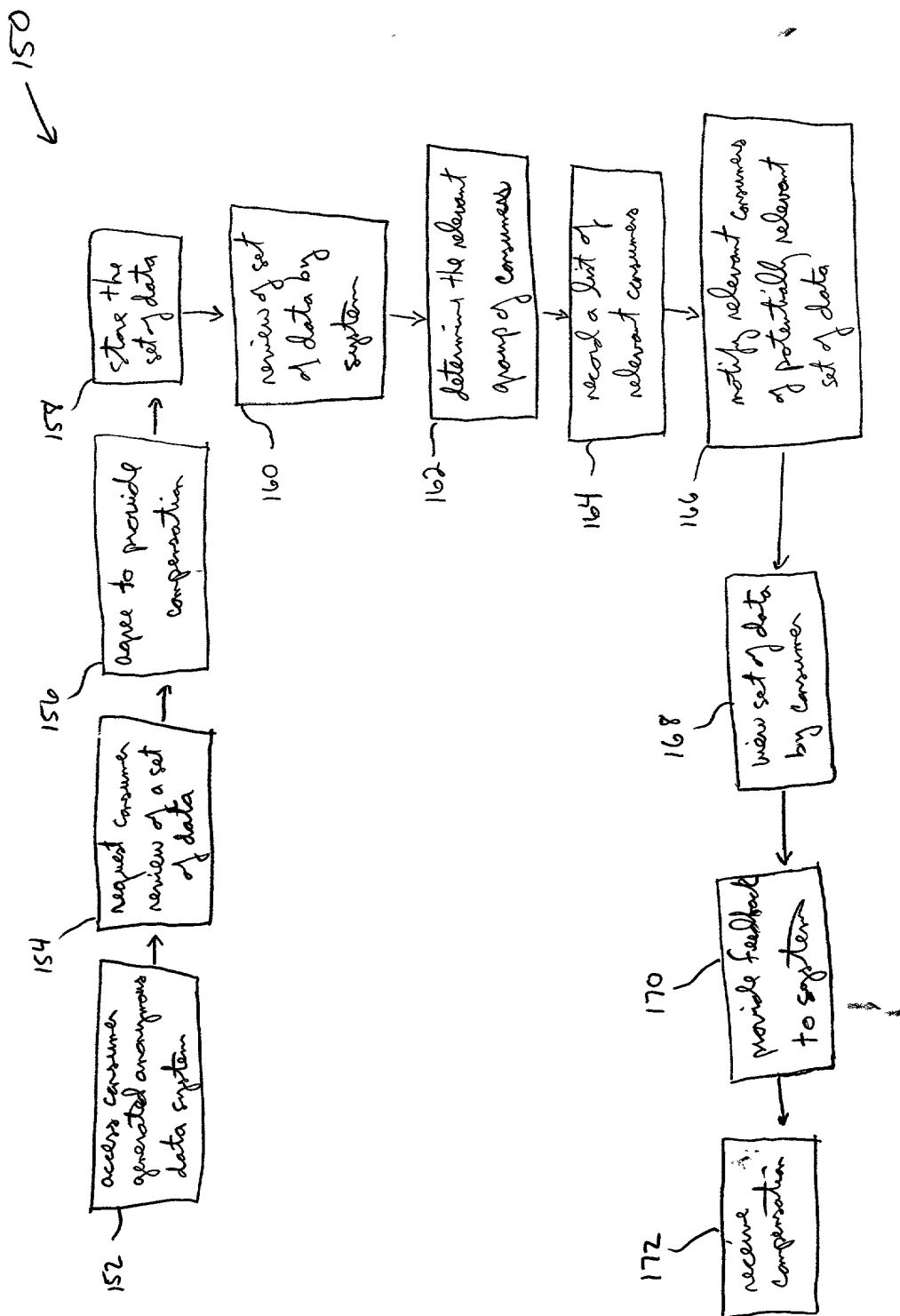
172 — receive compensation

DECLARATION AND POWER OF ATTORNEY	Attorney's Docket No. 10209-00007

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled: **METHOD AND APPARATUS FOR ANONYMOUS DATA PROFILING** the specification of which:

(check one)   [✓]   is attached hereto

                    [ ]   was filed on _____ as Application Serial No. _____,

                            and was amended on _____.

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations §1.56(a).

I hereby claim priority benefits under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112. I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

Application Serial No.	Filing Date	Status (patented, pending, abandoned)

I hereby claim the benefit under Title 35, United States Code §119(e) of any United States provisional application(s) listed below:

Application Serial No.	Filing Date	
		_____ Additional provisional application numbers are listed on a supplemental priority sheet attached hereto.

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. (*list name and registration number*)

John S. Beulick, Reg. No. 33,338; Patrick W. Rasche, Reg. No. 37,916; Michael Tersillo, Reg. No. 42,180; Alan L. Cassel, Reg. No. 35,842; Tara A. Nealey, Reg. No. 42,927; Elizabeth D. Odell, Reg. No. 39,532 and Bruce T. Atkins, Reg. No. 43,476, all of Armstrong Teasdale, One Metropolitan Square, Suite 2600, St. Louis, MO 63102-2740

Send Correspondence to: John S. Beulick Armstrong Teasdale LLP One Metropolitan Square, Suite 2600 St. Louis, MO 63102-2740	Direct Telephone Calls To: John S. Beulick 314/621-5070

DECLARATION AND POWER OF ATTORNEY	Attorney's Docket No. 10209-00007

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application and any patent issued thereon.

SOLE OR FIRST INVENTOR:

Full Name: __Eugene August Fusz__

Signature: _____   Date: __10/26/99__

Residence: __St. Louis, MO 63141__

Citizenship: __U.S.A.__

Post Office Address: __925 North Lindbergh, St. Louis, MO 63141__